English • Deutsch • Español • Français • Italiano • ??? • Polski • Português • ??????? • Svenska • ???(????)? • ???(??)? •

Contents

Introduction

This guide teaches you how to broadcast multiple WLAN SSID's using virtual interfaces. You can have different encryption settings for each WLAN and you can restrict what they have access to. You may also bridge a VLAN or VPN tunnel interface to the virtual wireless interface.

Note: Virtual Access Points (VAP's) and VLAN's are entirely different technologies and you should be careful not to confuse these terms. If you're referring to a virtual wireless interface then call it a VAP, if you're referring to an Ethernet VLAN then call it a VLAN, and if you bridge them together then say that you've bridged a VAP and VLAN.

Preparation

As with all configuration changes, it is best to connect your router with an Ethernet cable so that you do not get disconnected or locked out of your router while configuring it. If you wish to bridge a VLAN or other interface to the virtual wireless interface, then see other guides on how to set up those interfaces, this guide will just tell you how to bridge it.

If your router is configured as a Wireless Access Point (WAN is disabled) then you must be sure to set the gateway and local DNS as recommended in the WAP guide. This also applies to WDS client nodes (but not the main WDS node) which are bridged to another router that does routing for them. Keep your eye out for the places this guide gives alternative instructions for WAP's.

Before beginning, read Bug 1853 about a minor bug with bridge creation and a haphazard fix to the bug that was introduced in changeset 16181. This guide will NOT be changed to reflect the bridge creation changes until *recommended builds* are affected by the change.

Atheros Based Hardware

The Atheros VAP interface will be named ath0.1 instead of wl0.1 so just substitute this name in the instructions.

Broadcom Based Hardware (Very old)

Very early Broadcom based routers have radios that do not support or only partially support multiple WLAN's. You will need to telnet or SSH to the router and run this command on the router:

```
nvram get wl0_corerev
```

- If the number is 4 or less then the router is too old.
- If it is between 5 and 8 then it is capable of multiple SSID's but not multiple BSSID's, which means the wireless interfaces will all have the same MAC address so some devices might not recognize both WLAN's, and you will need to use a build that has a VINT wireless driver.
- If it is 9 or above then the router fully supports multiple WLAN's, each with their own BSSID (MAC address).

Ralink Based Hardware

The Ralink VAP interface will be named ra1 instead of wl0.1 so just substitute this name in the instructions.

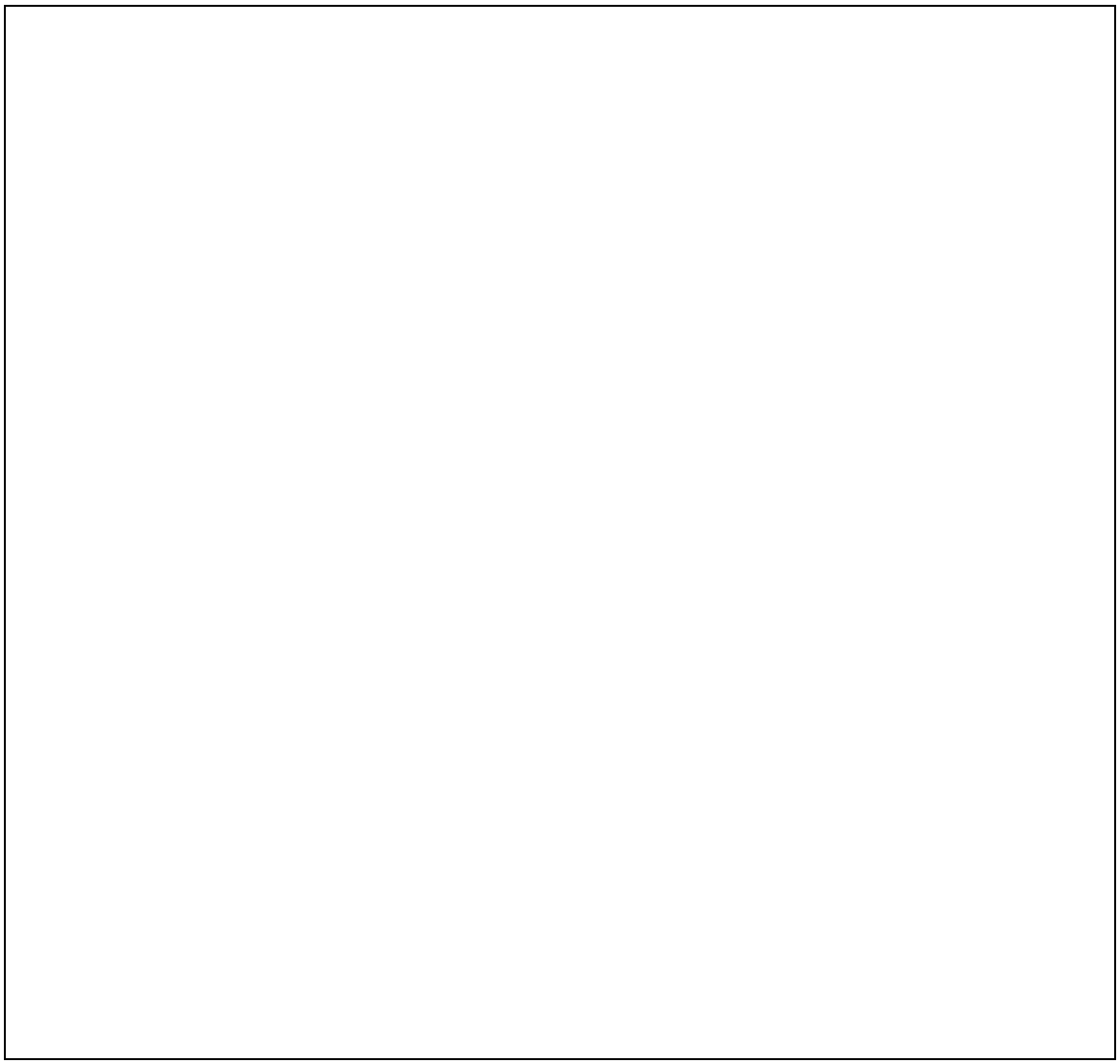
Configuration

GUI Method

Basic Wireless Settings

Use a web browser to connect to your router's web GUI. Navigate to the Wireless -> Basic Settings page and under the Virtual Interfaces section press the "Add" button to add a new virtual interface. Leave the Network Configuration set to "Bridged" for all interfaces regardless of whether you want to bridge them or not because "Unbridged" has unresolved bugs at the time this was written (svn 13312). To get a working unbridged interface we will actually assign it to its own bridge later on. You may change any of the other settings to your liking.

Although, as of around svn 30700, unbridging here works OK, at least for a single virtual interface, and even a part of specific firewall rules and dhcp/dns settings are automatically generated once you have set the 2nd dhcp server as explain below.



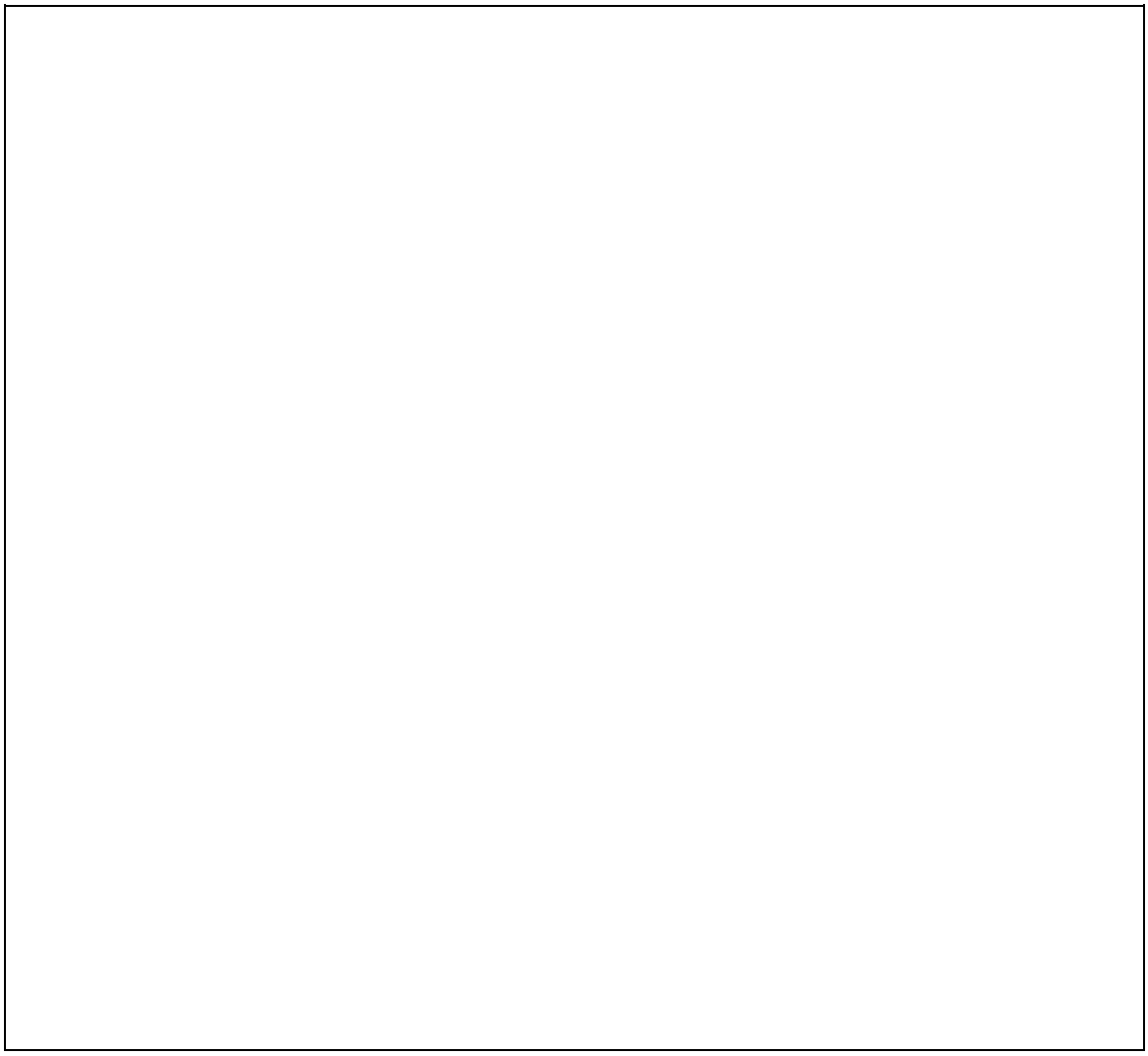
Press the "Apply Settings" button, wait 1 minute, and then you should be able to see and connect to your new WLAN SSID. Make sure that you can connect to it, receive a DHCP lease, and browse the network/internet before you do anything further.

Note: If you're using a Broadcom VINT build then some devices may have problems connecting. Often it is just that they will only display one SSID being broadcast but they will still be able to connect if you manually create a profile for the virtual interface's SSID. Two of my old 802.11g adapters can not see the VAP's SSID but can still connect with manual profiles while my 802.11n adapter can see both SSID's being broadcast.

Encryption

Configure whatever encryption you desire on the Wireless Security page. For instance, you may want WPA2-AES for your main interface to have maximum security but use WEP or no encryption on the virtual interface to allow others to connect. You may also use the same encryption type in order to have different passwords for different people.

Note: Firmware builds prior to 12548 are known to have trouble with using different encryption settings.



Press the "Apply Settings" button, wait 1 minute, and then you should be able to see and connect to both WLAN SSID's using their new encryption settings. Make sure that you can connect to both SSID's, receive a

DHCP lease, and browse the network/Internet before you do anything further.

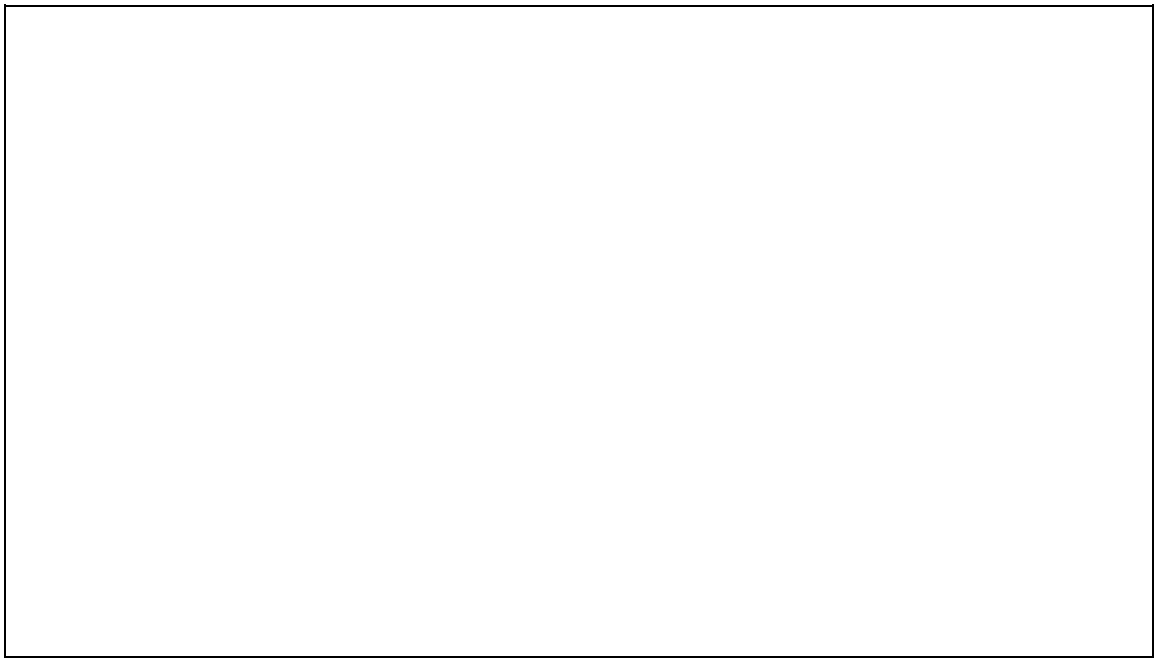
At this point you may stop if you want to allow everything to communicate together. If you are mixing strong encryption for your main network with weak encryption or none at all on the virtual interface then it is advisable to follow the steps below to separate the interfaces so that the virtual interface is restricted from communicating with your main network.

Separating the WLAN's

Navigate to the Setup -> Networking page. Press the "Add" button in the Create Bridge section and type "br1" into the blank input box that is on the left side of all the options that just appeared. Press the "Apply Settings" button at the bottom of the page and new input boxes will appear to specify the IP address for the new bridge.

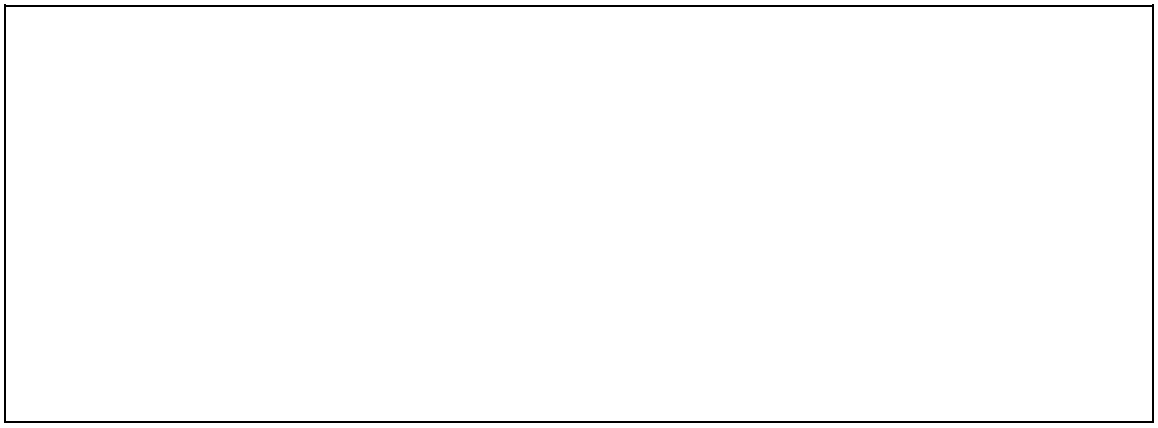
This new bridge needs to have an address that is in a different subnet than your main LAN. By default the main router LAN address is 192.168.**1**.1 netmask 255.255.255.0 so we will use 192.168.**2**.1 netmask 255.255.255.0 for the br1 bridge interface. Press the "Apply Settings" button again so that the IP address will be assigned to the br1 interface before you continue.

Note: (No longer true as of Oct 2016 on recent hardware, see link in this note below, but the following bug still exists in old hardware, eg wrt54gl with as of svn r30826) Would your netmask be different than 255.0.0.0, 255.255.0.0. or 255.255.255.0, you'll need to manually calculate the broadcast ip address of the subnet and set it via the startup script (see http://svn.dd-wrt.com/ticket/1406): when you set the bridge IP to 10.x.x.x, 172.<16to31>.x.x or 192.168.x.x, the broadcast IP will automatically be set respectively to 10.255.255.255, 172.<16to31>255.255. or 192.168.x.255 whatever the netmask you choose, which may be wrong. So, don't forget to add e.g. *brconfig br1 broadcast 10.11.12.47* for a 10.11.12.32/28 subnet in the startup script. You can use this online calculator to find it.... and manually run it on a command line once if you don't plan to reboot immediately. Reboot after setting the startup script is the advised way as some further changes "Apply" in the configuration may wipe the bridge broadcast ip.



Press the "Add" button in the Assign to Bridge section. Select "br1" in the left drop down menu that appeared and select "wl0.1" in the other. Press the "Apply Settings" button and the virtual wireless interface wl0.1 will now be moved from br0 to br1. If you wish to bridge a VLAN or other interface to the VAP, then you can add another bridge assignment to do so.

Press the "Add" button in the Multiple DHCP Server section. Select "br1" in the left drop down menu that appeared. Press the "Apply Settings" button to finish enabling the DHCP server for the br1 interface. (Take note that as of nov, 2016, Leasetime is in minutes)



Note: DHCP Type must not be set to "DHCP Forwarder," this type is often mistakenly used when it is not appropriate. If DHCP is disabled on your main LAN in Basic Setup because it is a WAP that connects LAN-LAN to an existing network instead of using the WAN port or DHCP is disabled for any other reason, then the Multiple DHCP method above will not work and instead you will need to use the Command Method for DHCP.

You should now be able to connect to VAP's SSID and receive a DHCP lease with an IP address that is in the 192.168.2.0/24 subnet. Make sure that you can connect to it, receive a DHCP lease, and connect to the router's 192.168.2.1 address from the VAP before you do anything further. On current builds (>17000) you will not be able to browse the internet until you add appropriate iptables commands later in the guide. If you are making a

WAP then you must either use the iptables commands for WAP's in the next section, or create routes throughout your network, or add a working tagged VLAN interface to the bridge.

Command Method

This section does not contain complete instructions. Currently it only has substitutions for the GUI method to overcome problems with certain configurations.

DHCP

Go to the Services tab and find the DNSMasq section. Make sure that DNSMasq is Enabled. Adjust the following options to fit your environment (omit the comment lines starting with '#') and put them in the **Additional DNSMasq Options** text area.

```
# Enables DHCP on br1
interface=br1
# Set the default gateway for br1 clients
dhcp-option=br1,3,192.168.2.1
# Set the DHCP range and default lease time of 24 hours for br1 clients
dhcp-range=br1,192.168.2.100,192.168.2.150,255.255.255.0,24h
```

Note: Seen in r28598 (24-dec-2015) and maybe before, the manual settings above are no more necessary: they all are set automatically when you create the bridge and the additional DHCP server parameters in the Separating the WLAN's section.

If you would like to use different DNS servers for the VAP then you can use this DNSMasq option regardless of which DHCP configuration method you used (NOTE: do not use brackets).

```
dhcp-option=br1,6,[DNS IP 1],[DNS IP 2]
```

July 2015 addition: Beside the info above (I didn't need to implement them as of build r25179), in a WAP setup hosting the DHCP server for the main LAN (br0) you may find the advertised dhcp options to the clients are wrong, at least the gateway (sent to client as WAP's lan IP). Paste this in the **Additional DNSMasq Options** text area:

```
option=lan,3,192.168.1.1      <-your gateway here
dhcp-option=lan,6,208.67.222.222,208.67.220.220       <-your prefered DNS servers here
```

Adapt to your needs (second line optional) These options seem to override the default wrong ones.

Restricting Access

Now that you have your WLAN's working you can start limiting what access they have. Here are several iptables commands that you can save to your firewall script on the Administration -> Commands page. These commands are written in the same order that the should appear in your firewall script, changing the order can affect the way that they work. Mix and match them however you like, just be sure to keep them in the order they appear on this page.

If you have any problems with your firewall script, then create a forum thread and be sure to describe in great detail what you're trying to do, what it is actually doing, and post your firewall script.

Enable NAT on the WAN port to correct a bug in builds over 17000 (doesn't make sense on WAP's)

```
iptables -t nat -I POSTROUTING -o `get_wanface` -j SNAT --to `nvram get wan_ipaddr`
```

Allow br1 access to br0, the WAN, and any other subnets (required if SPI firewall is on)

```
iptables -I FORWARD -i br1 -m state --state NEW -j ACCEPT
iptables -I FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu
```

Restrict br1 from accessing br0 (do not use on WAP's)

```
iptables -I FORWARD -i br1 -o br0 -m state --state NEW -j DROP
```

Restrict br0 from accessing br1

```
iptables -I FORWARD -i br0 -o br1 -m state --state NEW -j DROP
```

Restrict br1 from accessing the WAN port (no internet access!)

```
iptables -I FORWARD -i br1 -o `get_wanface` -j DROP
```

Restrict br1 from accessing the WAN subnet (still has internet, do not use on WAP's)

```
iptables -I FORWARD -i br1 -d `nvram get wan_ipaddr`/`nvram get wan_netmask` -m state --state NEW
```

Restrict br1 from accessing br0's subnet but pass traffic through br0 to the internet (for WAP's - WAN port disabled)

```
iptables -I FORWARD -i br1 -d `nvram get lan_ipaddr`/`nvram get lan_netmask` -m state --state NEW
```

Enable NAT for traffic being routed out br0 so that br1 has connectivity (for WAP's - WAN port disabled)

```
iptables -t nat -I POSTROUTING -o br0 -j SNAT --to `nvram get lan_ipaddr`
```

Force DNS redirection (for a WAP where you changed from Gateway to Router mode), e.g. to OpenDNS

```
iptables -t nat -I PREROUTING -i br1 -p tcp --dport 53 -j DNAT --to 208.67.220.222
iptables -t nat -I PREROUTING -i br1 -p udp --dport 53 -j DNAT --to 208.67.220.222
```

These 4 below are yet in recent builds:

Restrict br1 from accessing the router's local sockets (software running on the router)

```
iptables -I INPUT -i br1 -m state --state NEW -j DROP
```

Allow br1 to access DHCP on the router

```
iptables -I INPUT -i br1 -p udp --dport 67 -j ACCEPT
```

Allow br1 to access DNS on the router

```
iptables -I INPUT -i br1 -p udp --dport 53 -j ACCEPT
iptables -I INPUT -i br1 -p tcp --dport 53 -j ACCEPT
```

External Links

http://www.pennock.nl/dd-wrt/Multiple_BSSIDs.html - A command based guide.